MITRE | ATT&CK®

MITRE ATT&CK Framework

A Detailed Explanation of MITRE ATT&CK

Swipe →

What is the MITRE ATT&CK Framework?

The **MITRE ATTACK Framework** is a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework is meant to be more than a collection of data: it is intended to be used as a tool to strengthen an organization’s security posture. For instance, because MITRE ATT&CK takes the perspective of the adversary, security operations teams can more easily deduce an adversary’s motivation for individual actions and understand how those actions relate to specific classes of defenses.

Where does the data in the MITRE ATTACK Framework come from?

MITRE’s ATT&CK is populated mainly by publicly available threat intelligence and incident reporting, as well as by research on new techniques contributed by cyber security analysts and threat hunters. It is used by those same professionals to better understand the different ways bad actors might operate so adversarial behavior can be detected and stopped.

History of MITRE ATTACK Framework

MITRE is a nonprofit organization created to provide engineering and technical guidance to the federal government. The organization originally developed the framework for use in a MITRE research project in 2013 and named for the data it collects, which is Adversarial Tactics, Techniques, and Common Knowledge-or, in acronym form, ATT&CK.

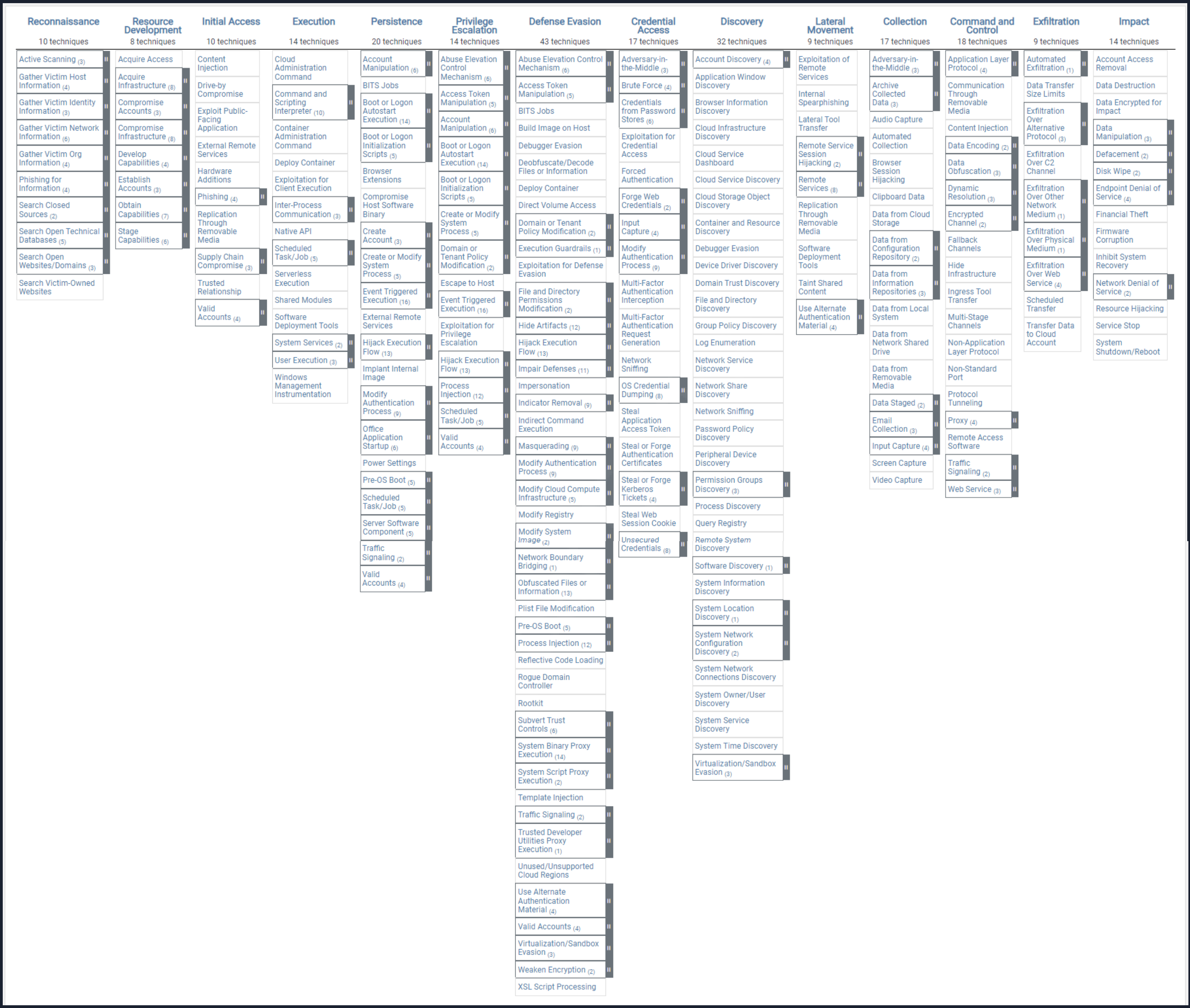
MITRE ATT&CK was released to the public for free in 2015, and today helps security teams in all sectors secure their organizations against known and emerging threats. And while MITRE ATT&CK originally focused on threats against Windows enterprise systems, today it also covers Linux, mobile, macOS, and ICS.

Here are three iterations of MITRE ATT&CK:

1. ATT&CK for Enterprise: Focuses on identifying and imitating adversarial behavior in Windows, Mac, Linux, and cloud environments.
2. ATT&CK for Mobile: Focuses on identifying and imitating adversarial behavior in Android and iOS operating systems.

3. ATT&CK for ICS: Focuses on describing the actions adversaries might take when they operate in an industrial control system (ICS).

The MITRE ATT&CK Matrix: tactics and techniques



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution (3)	Modify Authentication Process (9)	Scheduled Task/Job (5)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (13)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job (5)		Indicator Removal (9)	Unsecured Credentials (8)	Network Sniffing		Video Capture	Traffic Signaling (2)		
				Server Software Component (5)		Indirect Command Execution		Password Policy Discovery			Web Service (3)		
				Traffic Signaling (2)		Masquerading (9)		Peripheral Device Discovery					
				Valid Accounts (4)		Modify Authentication Process (9)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (13)		System Information Discovery					
						Plist File Modification		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (2)					
						Process Injection (12)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls (6)		Virtualization/Sandbox Evasion (3)					
						System Binary Proxy Execution (14)							
						System Script Proxy Execution (2)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

What are MITRE ATT&CK tactics?

Adversarial tactics are specific technical objectives that an adversary intends to achieve. Tactics are categorized according to these objectives. For instance, there are currently 14 tactics cataloged in the enterprise matrix:

✓ Reconnaissance: Techniques that actively or passively gather information to plan future targeted attacks.

✓ Resource development: Involves attackers purchasing or stealing resources to use them for a future attack.

✓ Initial access: Techniques where adversaries try to gain a foothold in your network through different attack vectors.

✓ Execution: Adversary techniques that try to run malicious code on a local or remote system.

✓ Persistence: Tactics that involve adversaries trying to maintain their foothold in your local or remote network.

✓ Privilege escalation: When an adversary tries to gain higher-level permission into your organization's network.

✓ Defense evasion: Adversary techniques to avoid detection when they move through your network.

✓ Credential access: Tactics focused on retrieving sensitive credentials such as passwords.

✓ Discovery: When adversaries try to gain an understanding of how your systems work.

✓ Lateral movement: Involves adversaries that enter and control systems, moving through your network.

✓ Collection: Techniques that gather information from relevant sources within your organization.

✓ Command and Control (C2 or C&C): When adversaries communicate with compromised systems to gain control.

✓ Exfiltration: Consists of techniques that straight up steal data from your network.

✓ Impact: When adversaries focus on disrupting data availability or integrity and interrupting business operations.

What are techniques?

A technique describes one specific way an adversary may try to achieve an objective. A multitude of techniques are documented under each "tactics" category. This is because adversaries may use different techniques depending on factors such as their skills sets, targets' system configuration and availability of suitable tools. Each technique includes a description of the method, the systems and platforms it pertains to, which adversary groups use it (if that is known), ways to mitigate the activity, and references to its use in the real world. MITRE ATT&CK currently identifies 188 techniques and 379 sub-techniques for enterprise.

What are some use cases of the MITRE ATT&CK Matrix?

Some of the ways a security team can use MITRE ATT&CK include:

- ✓ Conduct a security gap analysis and plan security improvements
- ✓ Strengthen cyber threat intelligence
- ✓ Accelerate Alert Triaging and Investigation
- ✓ Create more realistic scenarios for red team exercises and adversary emulations
- ✓ Assess maturity of security maturity of their SOC
- ✓ Communicate clearly and concisely to stakeholders
- ✓ Acquire a common language which is helpful when working with consultants and vendors